OFFICE OF THE CISO

Brian Contos
CISO Verodin

TOPIC: Evaluating New Security Solutions

with the Verodin Security Instrumentation Platform (SIP)

If you're not measuring overall security effectiveness when evaluating security products – you might be doing it wrong.

Objectively referee POC "bakeoffs" to see which security vendors work better for you

The most frustrating processes in evaluating security products is the proof of concept (POC). Call it a POC, bakeoff, pilot, evaluation, proof of value, trial, whatever, it's resource intensive. Also, if you are evaluating a new product against an existing one or multiple net new solutions at once or over time, it's slow and problematic to have an apples-to-apples comparison.

Once you've done your homework – which might include talking to industry analysts, reading third-party reviews, producing RFIs/RFPs, talking with references and reading through websites – it might be time to buy or it might be time for a POC. Regardless of endpoint security controls, firewalls, IPS, SIEMs, DLPs and related solutions, quality security vendors will want their solutions squarely compared to incumbents or new competitors in a thorough but fair evaluation.

Wouldn't it be nice to know exactly how a new control is going to work when compared to other controls – all in your environment, under the assault of real attacks, while integrated with your security management solutions – all in as little as an hour? That's where Verodin Security Instrumentation Platform (SIP) steps in so you can know exactly how your controls will respond to attacks.

There are many great security vendors that welcome the evaluation of their solutions. **If your vendor doesn't afford this option, that could be a warning sign.** A POC gives you a feel for how easy or hard it will be to deploy, configure, integrate and use the product in your environment. It also shows you the reality of the product as sometimes (not always, but sometimes) marketing and sales have stretched the art of the possible. How do you make your testing and evaluation fair across the various vendors and, more importantly, how do you do it quickly, easily and thoroughly?

Leveraging security solutions that demonstrate security effectiveness can prove to be very helpful during POCs.

Security instrumentation solutions like Verodin are commonly known to be used when evaluating your existing security effectiveness to address **questions like:**

- Are my **incident prevention** controls preventing attacks?
- Are my **incident detection** controls detecting attacks?
- Are my **SIEMs and log management** solutions collecting and correlating on these alerts?
- Is my **security team** prepared to respond?
- Are my **processes** designed to be efficient and effective?
- More simply put – is my security stuff **working the way I hope**, pray and assume it should?

This same level of scrutiny can be applied during POCs.

For example, you can evaluate the capabilities of an endpoint control, firewall, etc. By safely executing attacks across various security controls, Verodin SIP can see if your controls are blocking, alerting, etc. Verodin can also detect if the alerts show up in the solution's management console, then, further, do those events show up in your SIEM?

With Verodin SIP, you can run a variety of evaluations across endpoints and networks such as: malware execution, CLI attacks, PowerShell attacks, tunneling, data exfiltration, SQL Injection and C&C traffic.

These attacks can be safely executed across everything from existing security controls within the production environment to security controls deployed in a lab environment.

The results of the testing will provide an apples-to-apples comparison of how these security controls performed in the face a multitude of identical attacks. Did they block the attack, did they detect the attack, were they able to log that information to a SIEM, and, if it was logged to the SIEM, was the information valuable and usable?

Now, regardless of if you are evaluating the capabilities of your existing security controls against new controls, or multiple new controls against each other, you are armed with a valuable solution for evaluating security effectiveness that can yield results quickly.

Verodin provides a platform (SIP), so you can quickly, easily and thoroughly evaluate your security effectiveness.

Solid endpoint security, network security and security management vendors will welcome this level of analysis. Other vendors **may not** want you to know this option even exists.

Your security effectiveness should never be assumed.

You should have empirical evidence illustrating the value that your new solution will bring to your organization.

With Verodin SIP, you will quickly know exactly how a new control will work when compared to other controls – all in your environment, under the assault of real attacks, while integrated with your security management solutions.

About Verodin

Security Instrumentation Platform (SIP)

Verodin SIP is the first business platform to measure, manage and improve cybersecurity effectiveness. The revolutionary platform empowers enterprises to remove assumptions and prove their security effectiveness with quantifiable, evidence-based data. With Verodin SIP, you can observe and adjust real responses to real attacks without ever putting production systems in danger. Verodin customers dramatically increase the ROI of their existing security investments, achieve maximum value from future spending and measurably mature their cyber prevention, detection and response capabilities.

Learn more at verodin.com.

OFFICE OF THE CISO
About the author:

Brian Contos
VP, CISO Verodin

Brian Contos has over two decades of experience in the security industry. He is a seasoned executive, board advisor, security company entrepreneur and author. After getting his start in security with the Defense Information Systems Agency (DISA) and later Bell Labs, Brian began the process of building security startups and taking multiple companies through successful IPOs and acquisitions including: Riptech, ArcSight, Imperva, McAfee and Solera Networks.